F1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 January 2002 (10.01.2002)

PCT

(10) International Publication Number
WO 02/03178 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US01/17275

(22) International Filing Date: 29 May 2001 (29.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/607,375 30 June 2000 (30.06.2000) US

(71) Applicant: **INTERNET SECURITY SYSTEMS, INC.** [US/US]; 6303 Barfield Road, Atlanta, GA 30328 (US).

(72) Inventors: **IDE, Curtis E.**; 235 Nestor Court, Roswell, GA 30076 (US). **BRASS, Philip C.**; 1140 Pine Grove Pointe Drive, Roswell, GA 30075 (US). **DOTY, Theodore R.**; 540 Summerhill Drive, Roswell, GA 30075 (US).

(74) Agent: **PETTY, W. Scott**; King & Spalding, 191 Peachtree Street, Atlanta, GA 30303-1763 (US).

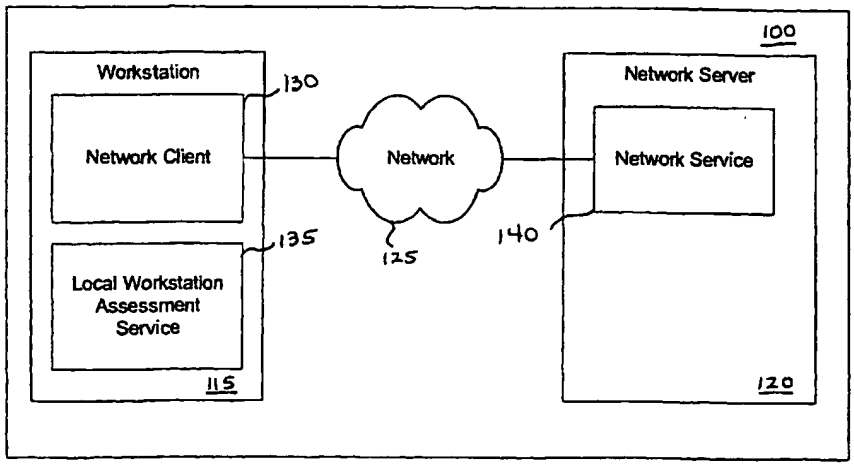
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND APPARATUS FOR NETWORK ASSESSMENT AND AUTHENTICATION



(57) Abstract: Providing a user with assurance that a networked computer is secure, typically before completion of the log-in operation. This can be accomplished by extending the local log-in process to perform a host assessment of the workstation prior to requesting the user's credentials. If the assessment finds a vulnerability, the log-in process can inform the user that the machine is or may be compromised, or repair the vulnerability, prior to completion of the log in operation. By performing vulnerability assessment at the level of the workstation, a network server is able to determine whether the workstation is a "trusted" platform from which to accept authentication requests. If the vulnerability assessment shows that the workstation is compromised, or if the possibility of remote compromise is high, the network server can elect to fail the authentication on the grounds that the workstation cannot be trusted. Optionally, a vulnerability assessment tool may be able to repair the vulnerability of the workstation, and then allow the authentication to proceed.

WO 02/03178 A2

METHOD AND APPARATUS FOR NETWORK ASSESSMENT AND AUTHENTICATION

FIELD OF THE INVENTION

The present invention relates to network security for distributed computer systems and, more specifically, to granting network services and determining the level of supplied services based upon an assessment of the vulnerability of a network computer.

BACKGROUND OF THE INVENTION

As use of network services becomes more prevalent in distributed computer networks, secure authentication of a computer user increases in importance. Authentication is required to prevent unauthorized use and abuse of network services. Authentication services typically require the user to verify his or her identity to the network service provider to determine whether that user is authorized to use a computer to access the network.

An authorization mechanism defines who is allowed to do what on a computer. Two computer authorization mechanisms for typical operating systems are privileges and object access control. Users granted a specific privilege can perform an action that is denied to users who do not have the privilege. Typically, privileges are not evaluated on a per-object basis. Instead, a privilege is applied in general to an action for a user. For example, the root user in most UNIX operating systems has a set of privileges associated with authorized actions. The "WINDOWS NT" operating system supports the grant of a set of privileges on a per-user or user group basis.

When access control is required for a particular object, such as a file, a form of authorization other than a general privilege can be used to define a permission to access the object on a per user basis. Object access control can specify, for each object, different access permissions for different users. For example, on a UNIX system, the "chmod" command allows the user to specify read, write, and execute permissions for the owner, the group, and the world. The "WINDOWS NT" operating system uses a discretionary access list that grants control permissions for different users.

Both authorization methods support the control of computer actions based on the identity of the user. The user's identity establishes the privileges and the

objects that she can access via a computer. Establishing the identity of the user is crucial to security and control in a computer network and is the role of the authentication process.

There are three branches of authentication technology in common use today to assist verification of the identity of the user. Shared secret (password) technology is one; public key technology is a second; and biometric technology is a third. Conventional authentication involves confirming the user's identity by (1) verifying a shared secret, such as a password, (2) using public/private key encryption and verifying that the user knows the private key, or (3) using unique biometric information about the user, such as fingerprints, retinal patterns, or voice prints. All three technologies revolve around the fundamental principle of credentials. A credential is information useful to establish the identity of a computer user. An authenticating service requests credentials from the user to support a decision about the identity of the user based on the credentials.

In many organizations and homes today, users operate a workstation, which makes requests for a network service available on a computer network. The workstation is important in authentication for two reasons. First, the workstation is a platform from which the user can access resources, including network services, on the network. Users authenticate and connect to network services from their workstations. Second, the workstation can be silently compromised by an unauthorized party. A "silent" compromise is one that the user cannot easily detect without the aid of external security auditing tools. Silent compromise is typically accomplished by installing a compromise tool called a "root kit" or a "backdoor" on the workstation. For example, current "hacker" software can be used to obtain the customer's password by logging keystrokes or browser screenshots can be taken to intercept SSL-protected HTTP traffic.

An intruder may compromise the integrity of a workstation, or a workstation may be misconfigured so that compromise is possible. The use of a network service may be compromised when a user accesses a network service from a compromised workstation. This subjects the network service to unauthorized use and abuse by the intruder on a valid user's workstation.

The effect of a compromised workstation is the potential violation of security mechanism that assumes the workstation is "trusted", including password-based authentication and some forms of biometric authentication. Smart card authentication implementations also can be subverted if the workstation's Trusted

Computer Base is subverted. For example, a user's credentials, such as password and biometric credentials, can be stolen or rogue code can be executed that impersonates the logged-on user.

Host assessment and authentication is relevant to the Internet environment because most Web clients are currently desktop machines. These machines are capable of being compromised, and are frequent targets of compromising attacks. Some Web sites attempt to verify the security of the client host by performing a security assessment before allowing transactions from that host.

For example, online banking applications are typically implemented by Web sites that allow customers to view account balances and pay bills. Customers and insurers want assurances that only the customer can perform transactions, and that the transactions are confidential. Current techniques include password authentication to verify that only the customer has access to their account, and SSL or PCT encryption to verify that there is no "man in the middle" capable of intercepting the network traffic.

In view of the foregoing, there is a need for a way for verifying the integrity of the workstation prior to granting access to and determining the level of a network service. The present invention solves the security compromise problem by providing assurances to the Web site operator (and their insurer) that the user's workstation has not been compromised or is easily compromised. The invention can accomplish this desirable objective by scanning the user's workstation for evidence of compromise and vulnerabilities that could lead to compromise. For example, when a user signs on to a Web site, the scan can be completed as part of the authentication process.

SUMMARY OF THE INVENTION

The disadvantages of the prior art are overcome by the present invention, which can restrict access to a network service based on information about the integrity and security posture of the workstation that originates the service request. A network service receives a request for service from a user on a workstation. Prior to authorizing access to the service, the network service requests or expects to receive credentials from the user and/or the workstation. Workstation credentials are presented as part of the authentication process, and typically include information about the current integrity of the workstation, and the security posture of the workstation. The security posture typically includes data that indicates the potential

for the workstation to be compromised. The network service makes a decision about whether to process the service request based on the user credentials and/or the workstation credentials. If the network service decides to process the request, it may elect, based on the workstation credentials, to provide a degraded service that is consistent with the perceived risk of workstation compromise.

The present invention provides an authentication process that can refuse access by a workstation to a network service based on the integrity and security posture of the workstation that originates the service request. This inventive process can be integrated with other authentication processes, particularly user authentication processes, to enhance the security provided by the authentication process. This augments the authentication and authorization processes of existing network services.

The present invention can also perform workstation assessments from multiple security perspectives, store the different results, use the assessments to grant or deny service access, and issue a report of these results to authorized users. The term "multiple security perspectives" means that workstation assessments may be performed at different network locations, and with different levels of access to the workstation by a workstation assessment service.

More particularly described, the present invention provides a network authentication system comprising an assessment service for assessing the vulnerability of a workstation that can be connected to a network server. The network server provides network service(s) over a computer network and requires authentication to maintain secure operations. A workstation is assessed, either locally or over the network, for security vulnerabilities. A workstation assessment service produces workstation credentials comprising integrity information and security posture information. Integrity information describes whether the workstation is compromised, while security posture information describes the workstation's potential for compromise, or security risk. The results of an assessment are compared to a workstation security policy to decide whether to allow network service and to define a level of network service to be supplied to the workstation.

The workstation assessment service can be located on the workstation, thereby providing a local workstation assessment service. In the alternative, the workstation assessment service can operate on a network machine other than the workstation, thereby providing a network-based workstation assessment service. The network service, upon receiving the service request from a network client operating on a workstation, requests workstation credentials from a local workstation

assessment service on the requesting workstation or via the network-based workstation assessment service. The network service can use a persistent store to cache workstation credentials and thereby prevent overly frequent reassessments of the workstation.

The workstation policy can be stored on a network server that hosts the network service. In the alternative, the workstation policy can be stored on a network server that is different from the server that hosts the network service. The workstation policy also can be stored on the workstation.

Typical distributed computing environment includes a workstation and a network server, each coupled to a computer network. A network client operates on the workstation, whereas a network service operates on the network server. For a representative scenario, the network service can request workstation credentials from a local workstation assessment service operating on the workstation. In turn, a network client, as part of the network client authentication process, can transmit the workstation credentials to the network service. The network service processes the workstation credentials based on workstation policy and decides whether to allow service to the network client.

For another aspect, the network service requests workstation credentials from a network-based workstation assessment service. In response, the network workstation assessment service provides workstation credentials to the network service to support the authentication process. The network service processes the workstation credentials and workstation policy to determine whether to allow service to a network client operating on the workstation.

For yet another aspect, the network service can transmit a security challenge to the network client. In response, the workstation assessment service transmits a reply that allows the network service to verify that the workstation assessment service has completed an assessment. This challenge/response may be implemented by the transmission of a shared secret, such as a pseudo-random number. The response may be generated by a one-way-function (such as MD5 or SHA1) performed on a concatenation of the challenge, the shared secret, and the results of the workstation assessment. The network service verifies that a program with knowledge of the shared secret produced the results of the workstation assessment. The network service can "trust" the results of a workstation assessment based on a positive verification result.

The network service may utilize the results of the workstation assessment to provide a degraded level of service to the workstation. The service level corresponds with the results in the workstation assessment result set. The level of service can be driven by a metric, such as a scalar score calculated by assigning a weight to each possible result, adding the weights for each result in the workstation assessment result set, and providing a score threshold for each possible level of service. If a score exceeds the score threshold for a particular level of service, then that level of service may not be granted by the network service. In the alternative, a scalar score can be calculated based upon a weighted average of a vulnerability for a workstation, each vulnerability assigned a predetermined priority. Consequently, the level of service can be associated with any conventional metric.

The service level also can be decided by utilizing techniques, such as artificial intelligence or expert systems, to make an intelligent analysis of the risk involved to the network service, service provider, and end user, given the workstation assessment results. For example, if a network service provides a service in distinct facets, each service facet may make a determination about degree of service provided, utilizing the results of the workstation assessment. When a network service provides data transport for network services, each higher-level network service may make a determination about the service level to be provided, utilizing the results of the workstation assessment, as provided by the data transport service.

In view of the foregoing, it will be understood that the present invention can grant access to the network services and determine the level of supplied services based upon an assessment of the vulnerability of a workstation coupled to a computer network. The advantages and implementation of the present invention will be described in more detail below in connection with the detailed description, the drawing set, and the attached claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the primary components of a network security system, including a local workstation assessment service on a workstation, in accordance with an exemplary embodiment of the present invention.

Figure 2 is a logical flowchart diagram illustrating an authentication process in accordance with an exemplary embodiment of the present invention.

Figure 3 is a diagram showing interactions between a workstation having a local workstation assessment service and a network server having a network service in accordance with an alternative embodiment of the present invention.

Figure 4 is a diagram illustrating a network security system including a workstation having a local workstation assessment service and a workstation security policy for completing a local authentication decision in accordance with an exemplary embodiment of the present invention.

Figure 5 is a block diagram illustrating the primary components of a security system including a workstation assessment service co-located with a network service in accordance with an exemplary embodiment of the present invention.

Figure 6 is a diagram showing interactions between a workstation, network server, and network workstation assessment server of a network security system in accordance with an exemplary embodiment of the present invention.

Figure 7 is a diagram showing interactions between a browser and a Web server in a Web-based security system in accordance with an exemplary embodiment of the present invention.

Figure 8 is a diagram showing multiple security perspective assessments invoked by network server through a workstation assessment proxy service in accordance with an exemplary embodiment of the present invention.

Figure 9 is a diagram showing interactions between a workstation having a local workstation assessment and a network server having a network service in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

In environments where computers are shared, users want an assurance that the computer they are logging-in to is secure, before completion of the log-in operation. This can be accomplished by extending the local log-in process to perform a local host assessment of the workstation prior to requesting the user's credentials. If the assessment finds a vulnerability, the log-in process can inform the user that the machine is or may be compromised, or repair an identified vulnerability, prior to completion of the log-in operation.

By performing vulnerability assessment at the level of the workstation, the network server is able to determine whether the workstation is a "trusted" platform from which to accept authentication requests. If the vulnerability assessment shows that the computer is compromised, or if the possibility of remote compromise

is high, the network server can deny authentication because the workstation cannot be trusted. Optionally, a vulnerability assessment tool may be able to repair the vulnerability of the workstation, thereby allowing the authentication to proceed.

For example, corporations that implement Virtual Private Networks (VPNs) typically allow people physically located outside corporate facilities access to the corporate network. While corporate computer systems staff can secure the machines physically located in corporate facilities, they cannot control machines located outside corporate boundaries. These external machines present a security risk. Even if the users of the external machines are benevolent, the machines may have been compromised silently. If this happens, the intruder on the external machine may use the VPN connection as a stepping-stone to unauthorized use of the corporate network. This risk can be addressed by extending the log-in process to include vulnerability assessment of the external host. If the vulnerability assessment fails, the external host is not allowed to connect to the network and the user of the external host is notified of the security risk. Another alternative is to automatically address the vulnerability (with the user's approval) by repairing an identified vulnerability, prior to completing the VPN log-in process. This technology can also be used to secure dial-up networking. The dial-up networking authentication process can be extended to include vulnerability assessment of the dial-in host.

As used in the description herein and throughout the claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise: the meaning of "a", "an", and "the" includes plural references, the meaning of "in" includes "in" and "on." Also, as used herein, "global computer network" includes the Internet. A "network service" includes any service that is made available over a distributed computer network. Exemplary embodiments of the invention are now described in detail in connection with the drawings. Referring to the drawings, like numbers indicate like parts throughout the views.

Figs. 1 and 2 illustrate a client-invoked vulnerability assessment of a workstation in which the workstation credentials are generated locally at the workstation. In other words, the vulnerability assessment is invoked at the client and the assessment is completed by a local workstation assessment service on the workstation. As shown in Fig. 1, an exemplary network security system 100 comprises a workstation 115 operating a local workstation assessment service in a network environment including a distributed computer network 125 and a network server 120. A network client 130 retrieves workstation credentials, typically

including workstation integrity information and workstation security posture information, from the local workstation assessment service 135 on the workstation 115. The local workstation assessment service 135 generates the workstation credentials by completing a local examination of the workstation 115. The network client 130, which also resides on the workstation 115, presents these credentials to a network service 140 on the network server 120 during an authentication process. The network service 140 decides whether to provide service to the workstation 115 via the network 125 based on the workstation credentials. Specifically, the network service 140 completes this decision-making process by evaluating the workstation against a workstation security policy. This allows the network service 140 to determine the extent to which the workstation 115 complies with its security policy. The network service 140 typically uses a policy compliance measurement to decide what, if any, service level to be the supplied to the workstation 115.

Turning now to Fig. 2, a logical flowchart diagram presents an illustration of the sequence of exemplary steps completed by an authentication process in connection with the local workstation assessment service in Fig. 1. The authentication process is invoked at the client and the assessment is completed by the local workstation assessment service residing on the workstation. The exemplary authentication process 200 begins in step 205 in response to a user initiating a log-in operation on a workstation coupled to a computer network. The workstation includes a local workstation assessment service maintained in memory to support the local generation of workstation credentials. The local workstation assessment service can generate the workstation credentials by completing vulnerability assessment of the workstation. In step 210, a network client residing on the workstation retrieves the workstation credentials from the local workstation assessment service. In addition, the network client can obtain user credentials in step 215 from a user credential database. The network client can provide both the workstation credentials and the user credentials to a network service via a computer network. The network service operates on a network server and is operative to determine whether to provide service to a workstation coupled to the computer network based upon workstation credentials. In step 220, the network service accesses a workstation security policy to support a determination of whether to provide service to the requesting workstation. In a separate decision-making process, the user credentials can be compared to a user credential database to further support secure computing operations.

The network service completes an authentication decision in step 225 by applying the workstation credentials to the workstation security policy. In the event that the credentials satisfy the workstation security policy, the network service permits operation of the requested service by the workstation in step 230. If the credentials satisfy only a portion of the workstation security policy, the network service can elect to allow the workstation to access a degraded level of service, as shown in step 235. On the other hand, the network service can elect to deny service to the workstation, as shown in step 240.

Fig. 3 provides an illustration of another alternative exemplary network security system for a computer network comprising one or more workstations and a network server. Similar to Figs. 1 and 2, Fig. 3 illustrates a client-invoked vulnerability assessment with a local assessment of the workstation. A workstation 305 comprises a network client 310 and a local workstation assessment service 315. The network server 320 maintains one or more network services 325. Each workstation 305 can access the network service 325 via a distributed computer network. Prior to a service request, the network client 310 issues a request for workstation credentials to initiate an authentication process. In response, the local workstation assessment service 315 completes the vulnerability assessment of the workstation 305 and returns workstation credentials to the network client 310. In this manner, the workstation assessment is completed by a local assessment service operating on the host computer rather than by a server-based assessment service operable to complete a remote scan of the workstation.

The network client 310 can transmit the workstation credentials and/or user credentials to the network service 325 via the distributed computer network. A typical authentication process is completed by evaluating credentials for a workstation. The network service 325 accesses a workstation security policy to evaluate the workstation credentials and to determine the level of service, if any, to be provided to the workstation 305. The workstation security policy can be maintained on the network server 320 or on a separate server, such as a network policy server or a directory server. The network service 325 can determine whether to allow the workstation 305 to access a network service based upon a comparison of the workstation security policy to the workstation credentials. The network service 325 notifies the network client 310 of the authentication results generated by a comparison of the workstation security policy to the workstation credentials. Although the exemplary network security system 300 completes a local assessment of the host

computer, the authentication decision is completed by a separate computer on the distributed computer network, namely the network server 320.

Fig. 4 illustrates an exemplary network security system 400 that makes a local authentication decision based on a vulnerability analysis completed on the host workstation. The network security system 400 operates in a traditional client-server environment to support the delivery of network services to a client via a remote server. The client invokes the vulnerability assessment, which results in a local assessment of the workstation to support an authentication decision at the client workstation. A workstation 405 has a local workstation assessment service 415 and a workstation security policy 420. The workstation 405 further includes a network client 410, which can be connected a network 425, such as the global Internet. A network server operating a network service 435 is also connected the network 425.

The network client 410 queries the local workstation assessment service 415 for workstation credentials. The network client 410 completes a policy compliance measurement by using the workstation security policy 420 and the workstation credentials. The network client 410 can then decide whether to use traditional user authentication with the network service 435. Other options include storing the workstation policy on a separate server and caching the workstation credentials on the network server. In this manner, there is no requirement to assess the workstation for each service request.

Fig. 5 illustrates an alternative exemplary network security system 500 for network service authentication comprising a network workstation assessment service resident at a network server. The architecture of the exemplary network security system of Fig. 5 is based upon a vulnerability assessment invoked by a network service and an assessment completed at the network server rather than at the local workstation. In contrast, the workstation assessment service operates on the host or local workstation in the exemplary network security system 100 of Fig. 1. Turning now to Fig. 5, a network client 530, operating on a workstation 515, presents user credentials and a request for service to a network server 520 via a distributed computer network 525. A network service 540, resident on the network server 520, requests workstation credentials from a network workstation assessment service 535. This service may reside on the network server 520, as shown in Fig. 5, or on another server (not shown) connected to the network 525. The network workstation assessment service 535 generates the workstation credentials by remotely examining the workstation 515 for actual or potential vulnerabilities to security violations. In

turn, the network service 540 can evaluate the workstation 515 by comparing the workstation credentials against a workstation security policy. Based upon this evaluation, the network service 540 will determine the level of service, if any, to be provided via the network 525 to the workstation 515. For example, if the network service 540 decides to allow service to the workstation 515, the network server 520 delivers the service via the network 525 for use by the network client 530.

An alternative exemplary network security system is shown in Fig. 6. The exemplary network security system supports a network service-invoked vulnerability assessment of a client workstation where the network workstation assessment service is operating on a server other than the network server providing the network service. Turning now to Fig. 6, the exemplary network security system 600 comprises a workstation 605, a network server 610, and a network workstation assessment server 615, each connected to a distributed computer network, such as the global Internet or an intranet. To obtain a service from the network server 610, a workstation 605 issues a request for service to the network server 610 via the distributed computer network. In response, a network service operating on the network server 610 issues a request for a workstation assessment. The network workstation assessment server 615 responds to the workstation assessment request by remotely completing a workstation assessment of the workstation 605 via the distributed computer network. The workstation assessment comprises a scan of the workstation 605 to identify possible security vulnerabilities of that computer and generates security credentials for the workstation 605. The network workstation assessment server 615 can send the workstation credentials to the network server 610 via the distributed computer network. In turn, the network server 610 compares the workstation credentials to a workstation security policy and decides whether to allow the workstation 605 to access the service available on the network server.

The exemplary network security system illustrated in Fig. 6 is similar to the network security system shown in Fig. 5, with the exception that the network workstation assessment service is operating on a server other than the network server providing a network service. In other words, the network server 610 in Fig. 6 is not responsible for completing an assessment of the potential vulnerabilities of the workstation requesting access to network service. Instead, the network server 610 relies upon a workstation assessment service operating on a separate server, the network workstation assessment server 615, to complete a remote scan of the workstation 605 via the distributed computer network. The network service operating

on the network server 610 uses the scan results provided by the network workstation assessment server 615 to determine whether to provide a particular service level to the requesting workstation 605.

An exemplary process 700 for Web-based network service authentication relying upon browser-based technology is shown in Fig. 7. Turning to Fig. 7, the process 700 is initiated by a browser 705, which operates on a workstation, requesting a log-in page from a Web server 710 via a distributed computer network, such as the Internet. The Web server 710 provides a service that requires authentication and log-in of a requesting workstation. The Web server 710 transmits a workstation assessment agent, which may be a Java applet, ActiveX control, browser plug-in, or other Web-based executable content, to the Web browser 705 in response to the log-in-request. Once installed at the browser 705, the workstation assessment agent generates workstation credentials based on a local examination of the workstation. For example, if the workstation assessment agent is implemented as a browser plug-in, the plug-in operates within the browser environment to complete a scan of the host computer. The results of this vulnerability scan represent workstation credentials. For the representative example shown in Fig. 7, the workstation assessment agent is implemented by a browser plug-in 705'.

The workstation assessment agent, i.e., the browser plug-in 705', transmits the workstation credentials to the Web server 710 via the computer network. An application on the Web server 710, typically a Web server CGI 715, compares the workstation credentials to a workstation security policy to decide whether the workstation is secure. Service by the Web server 710 is allowed if the Web server CGI 710 determines that the workstation is secure and the Web server 710 authenticates the user. If the Web server CGI 715 decides to continue, and the Web server 710 has not already authenticated the user, the server may now begin the user authentication process. There is a benefit to authenticating the user after completing a vulnerability analysis of the workstation – it is more difficult for an intruder to steal a user's credentials if the intrusion is detected and the user authentication process is terminated before the user presents their credentials.

Table I provides an overview of the primary network service authentication tasks completed for the Web-based operating environment of a workstation assessment agent operating on a workstation and a Web server, as shown in Fig. 7. The workstation assessment agent completes vulnerability assessment tasks and transmits the assessment results to the Web server. In turn, the Web server

determines whether to provide a network service to the workstation based on the assessment results.

Table I

1. The user of a workstation requests a log-in page from a Web server, typically by clicking a button or link on a Web page to begin the authentication process.
2. A browser, operating at the workstation, loads a host authentication page. The host authentication page contains a browser plug-in representing a workstation assessment agent.
3. The browser plug-in performs a host assessment scan of the workstation.
4. The browser plug-in sends the scan results via a secure link to a CGI script on the Web server.
5. The CGI script uses the scan results to decide whether to grant the host access to a network service at the Web server.
6. If the host is granted access, the CGI script redirects the browser to the next step in the authentication process, namely user authentication. If the host is denied access, the CGI script redirects the browser to a page that explains why the host cannot be granted access to the Web server. This page also describes what the user can do to bring the host into compliance so that access will be granted.

The exemplary Web-based process shown in Fig. 7 is supported by two separate components: (1) the browser plug-in 705' that performs the workstation assessment; and (2) the CGI script 715, which evaluates the scan assessment results and determines whether the host satisfies authentication requirements. The browser plug-in and the CGI script are representative embodiments of software routines that operate on the workstation and the Web server, respectively. The workstation assessment service is provided by the browser plug-in and implemented by a variety of different software routines, including a Java applet or an ActiveX control.

Likewise, the network service implemented by the CGI script can be implemented by other conventional Web-based executable software programs. Consequently, it will be understood that the present invention is not limited to a particular Web-based implementation, such as the representative exemplary embodiment illustrated in Fig. 7.

The workstation assessment agent, implemented as a browser plug-in 705', has two main functions: host assessment and communication of workstation assessment results. The host assessment is completed to determine whether the host is compromised. The browser plug-in 705' runs a series of checks, each looking for a particular security risk. Each check generates a scan result, which indicates whether a vulnerability risk is present at the workstation. The browser plug-in 705' then prepares assessment results for transmission to the Web server.

The browser plug-in 705' communicates the assessment results to the CGI script 715 operating on the Web server 710. This communication is preferably completed in a secure manner, between the workstation and the Web server, so that results cannot be intercepted by a third party. The communication also should be secure in such a way as to prevent the transmission of false information to the CGI script 715. This can be accomplished by the use of authentication or encryption technologies

For example, the communication between the browser plug-in 705' and the CGI script 715 can be completed by sending an HTTPS GET request with vulnerability assessment results stored as parameters of the GET request. The browser plug-in 705' generates a URL that uses HTTPS for confidentiality and contains the scan results as parameters. These parameters can be obfuscated by using shared secret encryption to prevent reverse engineering of the communications channel and to insure transmission only to appropriate servers.

The CGI script 715 receives scan results from Web clients, and decides, based on the results, whether to continue the authentication process. The script 715 responds to the scan results by redirecting the Web client, i.e., the workstation, to one of two different Web pages based on this decision. If the script 715 decides to allow authentication to continue, it redirects the browser 705 to a page that continues or completes the log-on process. If the script 715 decides to deny access, it redirects the browser 705 to a page that explains that service access is denied, why access is denied, and what can be done to obtain access to the requested service.

The CGI script 715 is preferably capable of receiving encrypted data comprising scan results from the browser plug-in 705', decrypting the data, and making a decision based on the results. The script 715 can assign a score to each different vulnerability identified by the browser plug-in 705'. When all results are received from the browser plug-in 705', the script 715 calculates a total score by adding the score assigned to each vulnerability. The total score is then compared by the script 715 against a maximum allowable score. If the total score is less than or equal to the maximum allowable score, authentication is allowed to proceed. If the total score is greater than the maximum allowable score, access by the browser 705 to the Web server 710 is denied by the script 715.

The Web-based design illustrated in Fig. 7 requires the server to decide, based on security assessment information from the client, whether or not to grant access, or possibly grant restricted access to a client workstation. In the alternative, the client can make that decision, given sufficient decision-making information from the server. For example, a browser operating on a workstation can issue a request for a log-in page to a network server. In response, the network server can transmit the log-in page, an authentication plug-in, and a workstation policy to the workstation via the computer network. The authentication plug-in is installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network. The workstation security credentials can be compared to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network.

In most web service contexts, the result of a decision-making process for determining whether to grant access by a client to a network service can be expressed as making a choice between URL's. If the decision comes out one way, the browser points to one URL. If it comes out another way, the browser points to a different URL. This can be accomplished on the server side by instructing the client to submit scan information to the server, and having the server redirect the client to the appropriate URL after making the service access decision.

The client's decision-making procedure typically involves three types of information: vulnerability weights, used to calculate a host score based on found vulnerabilities, a "max score", used to gate service, and two URLs, one for passing scores and one for failing scores. If the host's score exceeds the max score, the host is

not granted access, and is redirected to the URL for failing scores. If the host's score is less than or equal to the max score, the host is allowed access, and is redirected to the URL for passing scores.

A network server can send vulnerability weights, max score, and URLs to the client, thereby allowing the client to calculate the host score, compare it to the max score, and redirect the browser to the appropriate URL. This delivery of information to the client via the computer network can be completed without compromising the consumer's privacy. However, if the URLs are transmitted to the client without protection, the consumer could intercept the transmitted URL and thereby circumvent the process.

By authenticating the control or plug-in transmitted to the web server, a verification can be completed so that only the control (or someone who knows the shared secret embedded within it) can request the "success" URL successfully. Assume that the "success" URL is actually the URL of a web script and that a crypto "challenge" is generated and passed to the control along with the URLs. The control can use this challenge, along with a shared secret known only to the control and the "success" URL web script, to generate a crypto "response".

Instead of redirecting the browser directly to the web script, the control can redirect the browser to the web script and pass the crypto "response" to the script (typically by simply appending it to the end of the URL). If the crypto "response" does not match the crypto "challenge" that was sent to the control, the script could redirect the browser to the "failure" URL. This way, only those with knowledge of the shared secret (preferably only the control) can request the "success" URL and gain access. This client-based design requires the control to make the network service access decision, instead of sending information from the browser-based control to support a decision by the web server.

Fig. 8 illustrates an exemplary network security system having a workstation assessment proxy service for processing workstation assessment results. The exemplary network security system supports a vulnerability assessment invoked by a network service and a workstation assessment completed via a proxy service typically operating on a proxy server. As shown in Fig. 8, a network workstation assessment proxy service 815 collects workstation assessment information from a variety of sources with security perspectives at the request of a network service 810 or a network client 820. This proxy service 815 communicates with different workstation assessment services, combines the assessment results, and returns the

results to the network service. The different workstation assessment services can reside, for example, on a local workstation, on the Internet, on a LAN, or on a WAN. The assessment results can be cached in storage for subsequent use. These workstation assessment services provide assessments of the workstation that show security weaknesses visible for a particular level of authentication (i.e. administrative access, guest/anonymous access, normal user level access, etc.). This information can be used by the network service 810 to form a more complete estimate of the workstation's security posture and risk profile.

The exemplary network security 800 operates in a distributed computing environment comprising a workstation 805, a network service 810, a workstation assessment proxy service 815, a LAN-based network assessment service 830, and an Internet-based network assessment service 835. The distributed computing environment can include one or more workstations 805, each including a network client 820 and a local workstation assessment service 825. An authentication process is initiated in response to network client 820 generating a service request via the distributed computer network. The network service 810 responds to the service request by issuing a workstation assessment request to the workstation assessment proxy service 815. In turn, the workstation assessment proxy service 815 will issue multiple assessment requests to a variety of assessment services to evaluate the potential vulnerability of the workstation 805.

For example, the workstation assessment proxy service 815 can issue a local assessment request to the local workstation assessment service 825 via the distributed computing network. In addition, the workstation assessment proxy service 815 can issue a network assessment request to both the LAN-based network assessment service 830 and the Internet-based network assessment service 835. Each assessment service completes a scan of the workstation 805 and returns assessment results to the workstation assessment proxy service 815 via the distributed computing network.

In turn, the workstation assessment proxy service 815 can combine the assessment results and transmit the combined assessment results to the network service 810 via the distributed computer network. The network service 810 applies a workstation security policy to the combined assessment results to determine the level of service, if any, to be provided to the requesting workstation 805. The workstation security policy can be maintained on the network server hosting the network service or a separate server, such as a network policy service or a directory server. The

network service 810 notifies the network client 820 of the authentication results via the distributed computing network.

Another alternative exemplary network security system is shown in Fig. 9. The exemplary network security system supports a vulnerability assessment invoked by a network service and an assessment completed at the local worktation. The exemplary network security system 900 comprises a workstation 905 and a network server 910, each connected to a distributed computer network, such as the Internet or an intranet. The workstation 905 includes a network client 915 and a local workstation assessment service 920. The network server 910 includes one or more network services 925. To obtain a service from the network server 910, the network client 915 issues a service request to the network server 910 via the distributed computer network. In response, the network service 925 generates a request for an assessment of the workstation 905. The local workstation assessment service operating on the workstation 905 responds to the assessment request by completing a vulnerability scan of the workstation 905 and generating workstation credentials. In turn, the local workstation assessment service 920 transmits the workstation credentials to the network service 925 via the distributed computer network. The workstation credentials represent an evaluation of workstation integrity and security posture.

The network service 925 assesses a workstation security policy, typically maintained at the network server 910, to evaluate the workstation credentials. Specifically, the network service 925 compares the workstation credentials to the workstation security policy to determine the level of service to be provided, if any, to the workstation 905. Although the workstation security policy is preferably maintained on the network server 910, it will be appreciated that the security policy also can be maintained on a separate server, such as a network policy server or a directory server. Based upon the evaluation of workstation credentials, the network service 925 issues a message to notify the network client 915 of the service level to be provided by the network service 925.

In view of the foregoing, it will be appreciated that an authentication process can be implemented at a Web server, which evaluates the access of a Web service by a workstation based on workstation credentials (security posture and integrity information). The user can not log-on to the Web service unless the workstation's security posture and integrity comply with the Web service's security policy. Alternately, the user receives a level of access appropriate to the degree of

compliance of the workstation's security posture and integrity with the Web service's security policy.

Alternatively, an authentication process can be implemented by a network connection. This prevents a workstation from joining a network without presenting workstation credentials for approval. This authentication process can be used when a workstation connects to a VPN or to a Microsoft Windows Domain.

The authentication process also can be implemented as an extension to an extensible authentication process, such as GSSAPI or Microsoft SSPI. Any network service that uses the extensible authentication process can validate the security of the workstation.

The authentication process can be implemented on a dial-up networking server. When a client dials up, the dial-up server validates the workstation credentials of the dialing up workstation, and decides whether to allow the call to continue or to allow degraded access to the dial-up services.

The present invention includes a Web-based system can be used for gathering, storing and presenting workstation assessment results. This system performs workstation assessments from multiple security perspectives, and stores the results in a database server. Authorized parties may later retrieve these results by connecting to the Web server. The Web server operates a Web application that grants access to the data in the database for each workstation, and provides Web reports to authorized parties. Because the system stores workstation assessment results from multiple network location and authentication perspectives, it is capable of presenting a comprehensive view of workstation security posture. This comprehensive view can include internal and external assessments of the workstation.

The present invention is directed to network security for distributed computer systems, including the client-server computing environment. Those skilled in the art will appreciate that a server can operate as a client in a server-to-server environment. In other words, the first server can be a "client" of another server in the distributed computer network. This being the case, the role of the "workstation" described throughout this document can be fulfilled by a server that is requesting access to a network service. Thus, that server would then be assessed via the workstation assessment process during the authentication process. Typically, when one server connects to another server, user credentials, if required, are provided by a computer program or process rather than by a computer user. This use of user authentication and credentials for allowing access by a computer program or process

follows the same purpose and method as that of a computer user and, as such, fits within the confines of user authentication as described in this document. Moreover, a client can be implemented by a conventional desktop computing device, a mobile computing device, and other computing platforms, such as browser-enabled telephony devices and personal digital assistants (PDAs).

Significantly, the present invention can complete a vulnerability analysis of a workstation prior to completion of an authentication of the user of that workstation. A vulnerability analysis for the workstation is completed prior to user authentication because it is more difficult for an intruder to steal a user's credentials if the intrusion is detected and the user authentication process is terminated before the user presents their credentials to the workstation. Consequently, user credentials are preferably compared to a user credential database, which is typically maintained on a server separate from the workstation, only after completion of a vulnerability analysis of the workstation. Those skilled in the art will appreciate, however, that a vulnerability analysis of the workstation can also be completed after user authentication has been successfully completed. For example, the vulnerability assessment can be completed after user authentication and prior to substantive operation of a network service at the workstation.

The above-described embodiments are presented as illustrative examples. It will be readily appreciated that deviations may be made from the specific embodiments disclosed in this specification without departing from the invention. Accordingly, the scope of this invention is to be determined by the claims below rather than being limited to the specifically described embodiments above.

CLAIMS

What is claimed is:

1. A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

generating workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and

authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation.

2. The computer-implemented process recited by Claim 1 further comprising the step of authorizing access to a predetermined level of the network service if the workstation security credentials satisfy a portion of the workstation security policy.

3. The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a local workstation assessment service maintained on the workstation, the local workstation assessment service operative to generate the workstation security credentials.

4. The computer-implemented process recited by Claim 3, wherein the workstation security policy is maintained on the workstation, the process further comprising the step of providing the workstation security credentials from the local workstation assessment service to the workstation security policy.

5. The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a network workstation assessment service maintained on the network server, the network workstation assessment service operative to generate the workstation security credentials.

6. The computer-implemented process recited by Claim 5, wherein the workstation security policy is maintained on the workstation, the process further comprising the step of providing the workstation security credentials from the network workstation assessment service to the workstation security policy on the workstation via the computer network.

7. The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a network workstation assessment service maintained on an assessment server coupled to the computer network, the assessment server operating as a remote server different from the network server, the network workstation assessment service operative to generate the workstation security credentials.

8. The computer-implemented process recited by Claim 7, wherein the workstation security policy is maintained on the network server, the process further comprising the steps of:

transmitting the workstation security credentials from the network workstation assessment service on the assessment server to the network service on the network server via the computer network; and

comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service.

9. The computer-implemented process recited by Claim 8 further comprising the step of communicating a service decision from the network server to the workstation via the computer network, the service decision defining whether the workstation is allowed to access the network service or a degraded form of the network service.

10. The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by the network service on the network server in response to receiving a request for the network service from the workstation via the computer network.

11. The computer-implemented process recited by Claim 10, wherein the workstation security policy is maintained on the network server, the process further comprising the step of comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service or a degraded form of the network service.

12. A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; and

a workstation security policy, operative on the workstation, for defining security policy requirements for secure operations by the workstation;

the local workstation assessment service further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service,

the local workstation assessment service further operative to authorize access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy.

13. A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network; and

a network service, operative on the network server, for determining whether the workstation should be granted access to a software service of the network service in response to receiving the workstation security credentials via the computer network.

14. The network security system recited by Claim 13 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

15. The network security system recited by Claim 14, wherein the network service is further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy.

16. A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

the network service operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

the network service further operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials.

17. The network security system recited by Claim 16 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

18. The network security system recited by Claim 17, wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy.

19. A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a log-in page to a network server from a browser operating on the workstation;

transmitting the log-in page and an authentication plug-in from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and

determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials.

20. The computer-implemented process recited by Claim 19 wherein the step of determining whether the workstation should be granted access to the software service comprises the step of the CGI script comparing the workstation security credentials to a workstation security policy maintained at the network server to determine whether the workstation should be granted access to the software service;

if the workstation security credentials satisfies the workstation security policy, then authorizing access to the software service and directing the browser to the log-in page via the computer network,

otherwise, denying access to the software service and delivering an access denied page to the workstation via the computer network.

21. A network security system for authenticating a workstation requesting a network service operating on a network server via a computer network, comprising:

a network assessment service operating on a network workstation assessment server on the computer network, the network assessment service operative to generate workstation security credentials by completing a vulnerability assessment of the workstation via the computer network to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network,

the network service, responsive to receiving the workstation security credentials from the network assessment service via the computer, operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials and the user credentials.

22. The network security system recited by Claim 21 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

23. The network security system recited by Claim 22, wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials and the user credentials satisfy the workstation security policy.

24. The network security system recited by Claim 21, wherein the network service is operative to transmit to the network assessment service via the computer network a request to complete the vulnerability assessment of the workstation in response to receiving a request for the software service from the workstation.

25. A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a log-in page to a network server from a browser operating on the workstation;

transmitting the log-in page, an authentication plug-in, and a workstation policy from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

comparing the workstation security credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network.

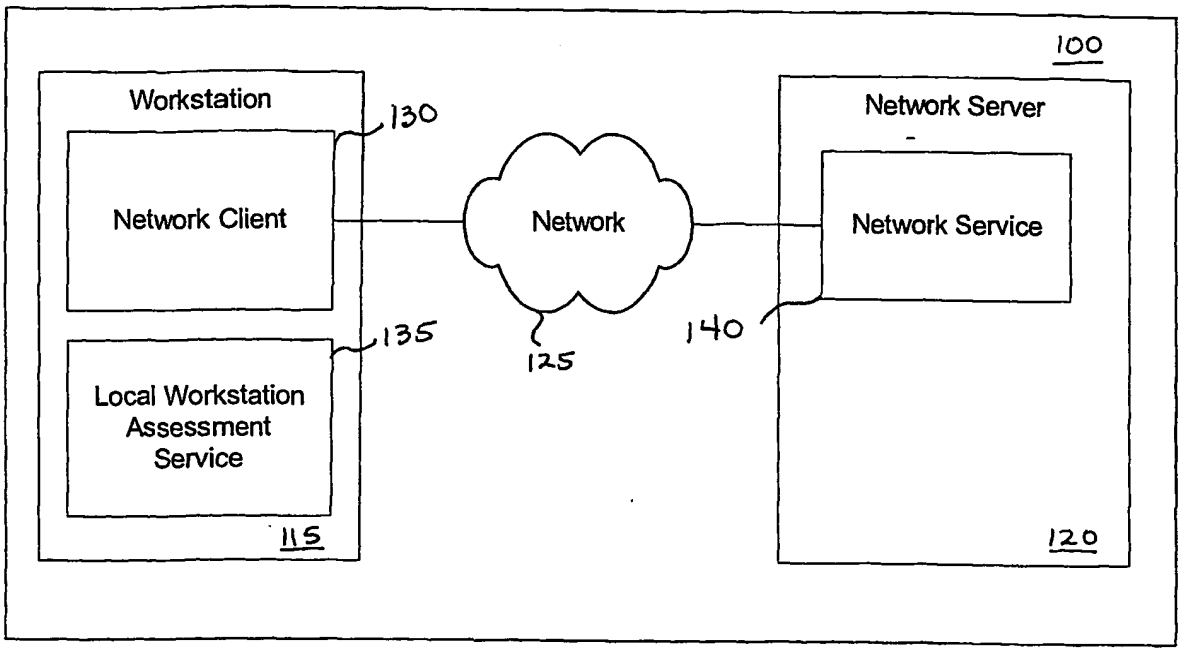

100
Workstation
130
Network Client
Network
Network Server
Network Service
135
Local Workstation Assessment Service
125
140
115
120

Figure 1

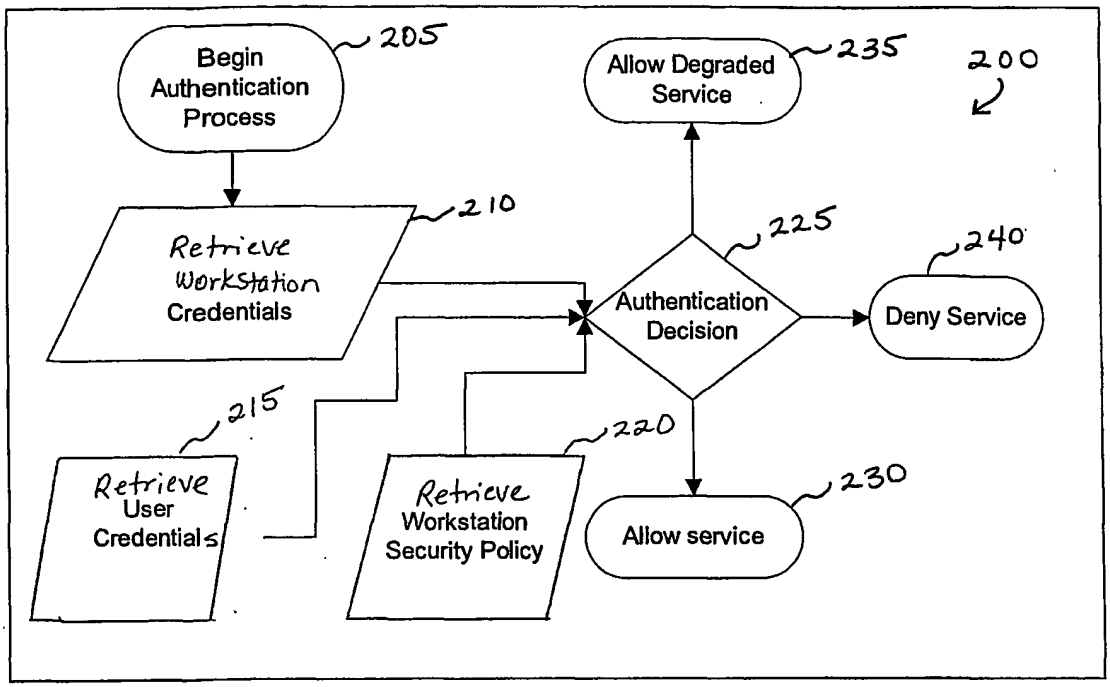

Begin Authentication Process
205
Allow Degraded Service
235
200
Retrieve Workstation Credentials
210
225
240
Authentication Decision
Deny Service
215
220
230
Retrieve User Credentials
Retrieve Workstation Security Policy
Allow service

Figure 2

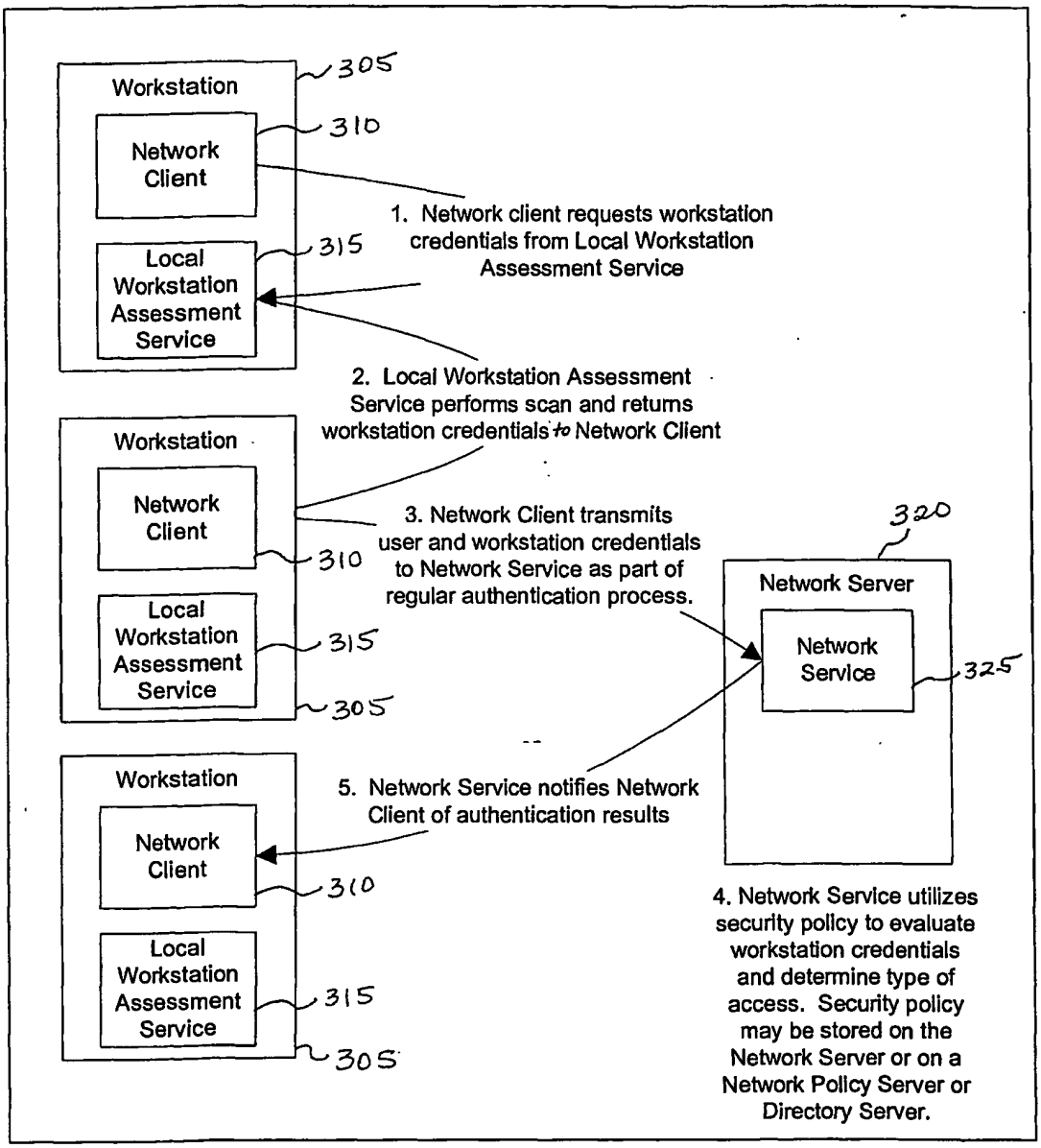

Workstation
305
Network Client
310
Local Workstation Assessment Service
315
1. Network client requests workstation credentials from Local Workstation Assessment Service
2. Local Workstation Assessment Service performs scan and returns workstation credentials to Network Client
3. Network Client transmits user and workstation credentials to Network Service as part of regular authentication process.
Network Server
320
Network Service
325
4. Network Service utilizes security policy to evaluate workstation credentials and determine type of access. Security policy may be stored on the Network Server or on a Network Policy Server or Directory Server.
5. Network Service notifies Network Client of authentication results

Figure 3

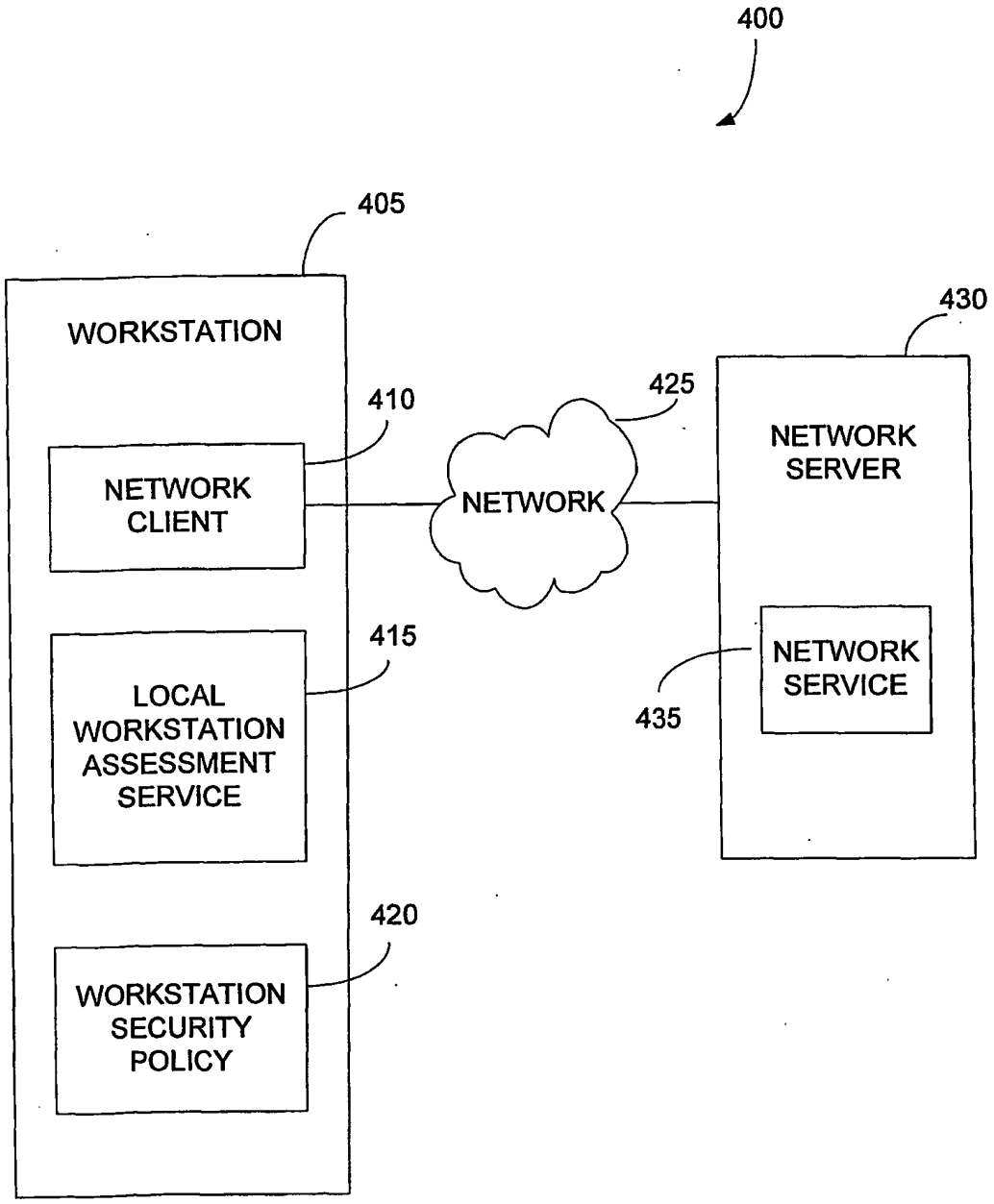

400
405
WORKSTATION
410
NETWORK CLIENT
415
LOCAL WORKSTATION ASSESSMENT SERVICE
420
WORKSTATION SECURITY POLICY
425
NETWORK
430
NETWORK SERVER
435
NETWORK SERVICE

Fig. 4

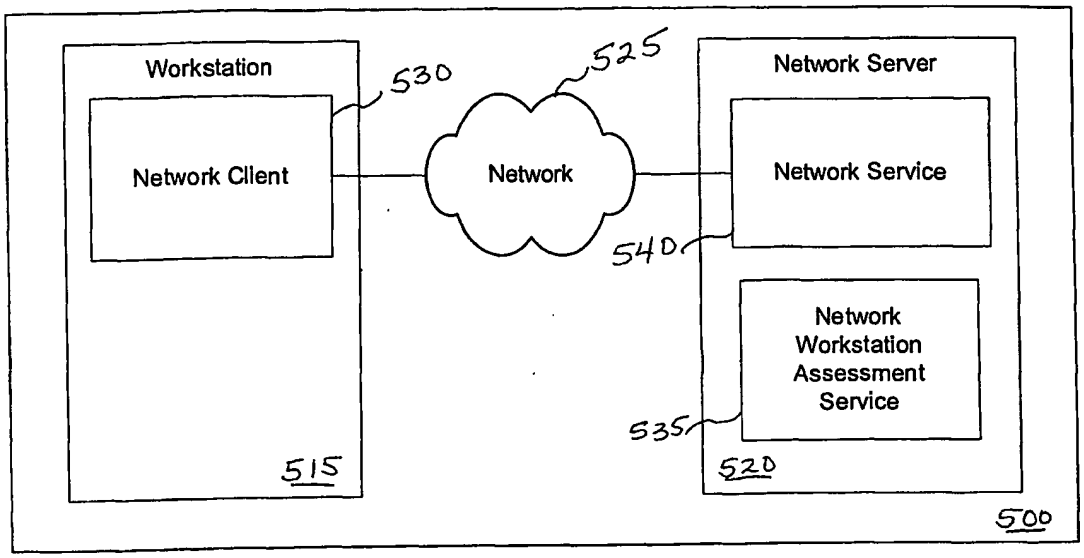

Workstation
530
525
Network Server
Network Client
Network
Network Service
540
Network
Workstation
Assessment
Service
535
515
520
500

Figure 5

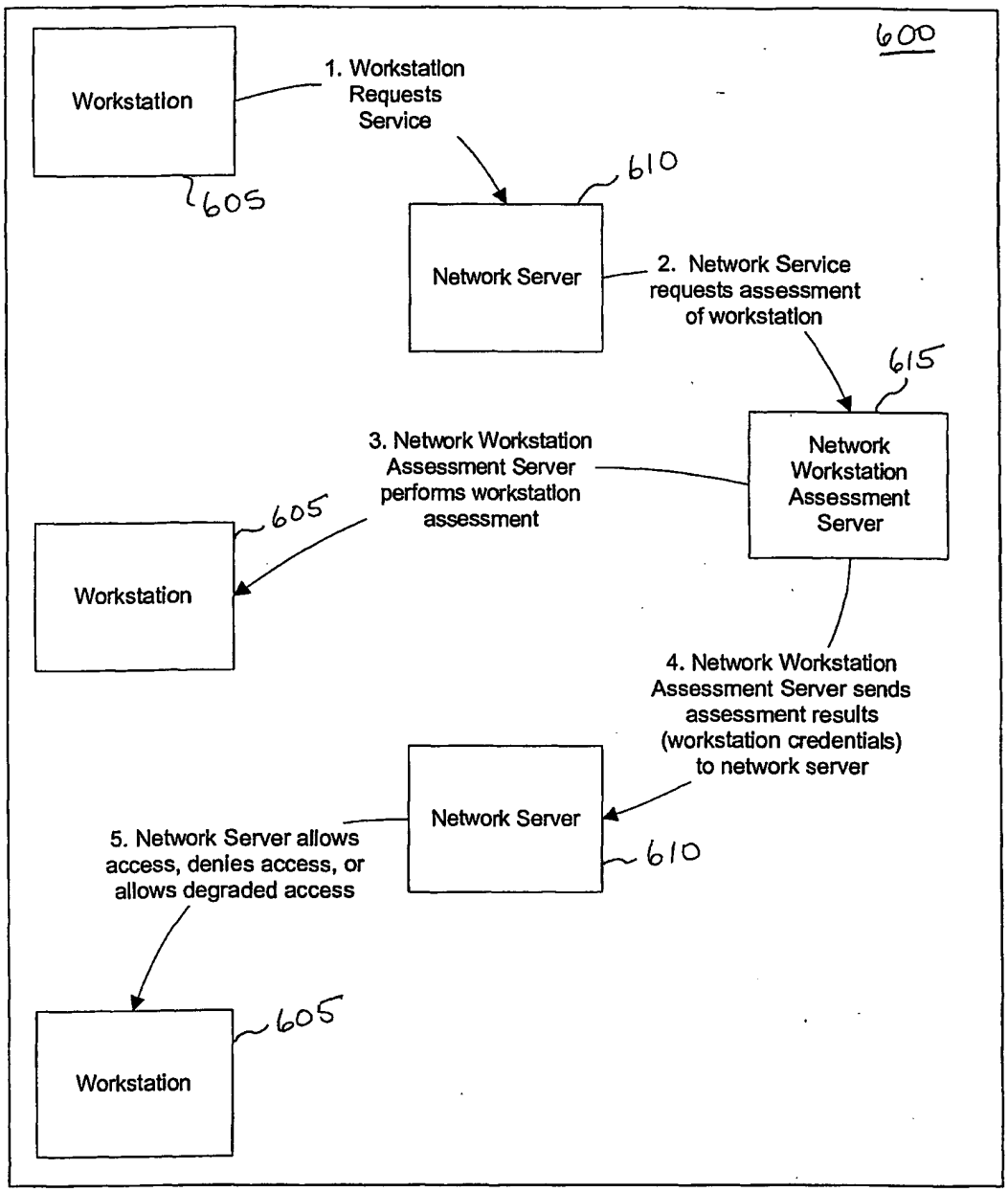

600
Workstation
1. Workstation Requests Service
605
610
Network Server
2. Network Service requests assessment of workstation
615
Network Workstation Assessment Server
3. Network Workstation Assessment Server performs workstation assessment
605
Workstation
4. Network Workstation Assessment Server sends assessment results (workstation credentials) to network server
Network Server
610
5. Network Server allows access, denies access, or allows degraded access
605
Workstation

Figure 6

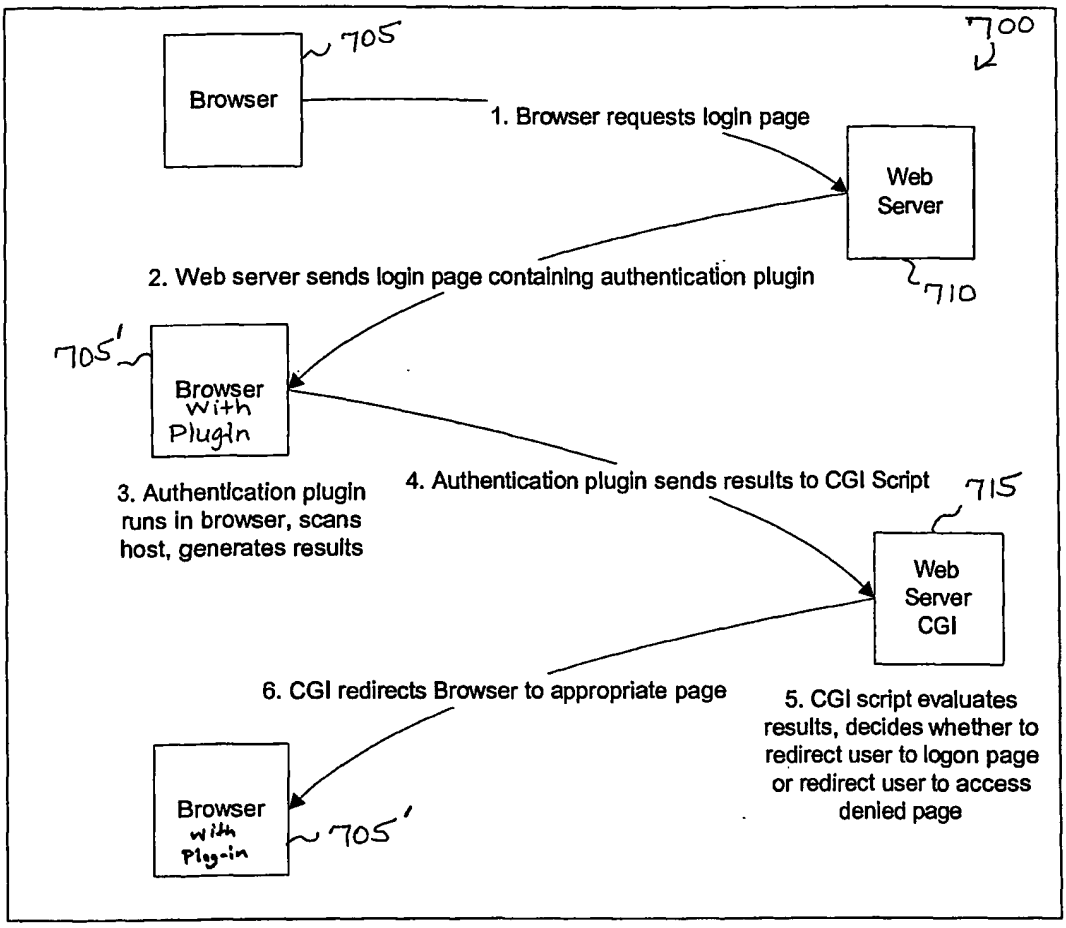

700
Browser
705
1. Browser requests login page
Web Server
710
2. Web server sends login page containing authentication plugin
705'
Browser with Plugin
3. Authentication plugin runs in browser, scans host, generates results
4. Authentication plugin sends results to CGI Script
715
Web Server CGI
6. CGI redirects Browser to appropriate page
5. CGI script evaluates results, decides whether to redirect user to logon page or redirect user to access denied page
Browser with Plug-in
705'

Figure 7

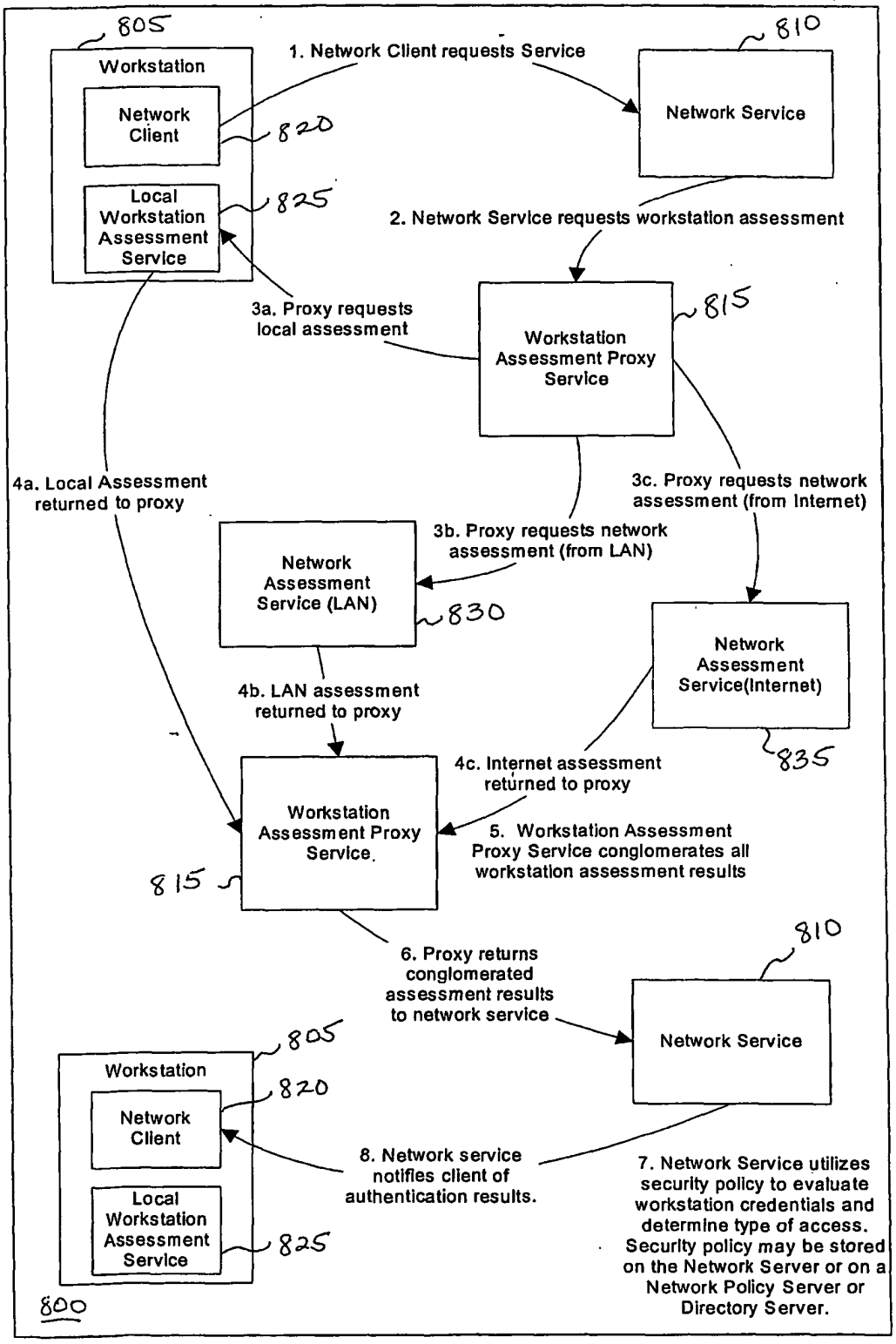

805
Workstation
Network Client
820
Local Workstation Assessment Service
825
1. Network Client requests Service
810
Network Service
2. Network Service requests workstation assessment
3a. Proxy requests local assessment
Workstation Assessment Proxy Service
815
4a. Local Assessment returned to proxy
3c. Proxy requests network assessment (from Internet)
3b. Proxy requests network assessment (from LAN)
Network Assessment Service (LAN)
830
Network Assessment Service(Internet)
835
4b. LAN assessment returned to proxy
4c. Internet assessment returned to proxy
Workstation Assessment Proxy Service.
815
5. Workstation Assessment Proxy Service conglomerates all workstation assessment results
6. Proxy returns conglomerated assessment results to network service
810
Network Service
805
Workstation
820
Network Client
8. Network service notifies client of authentication results.
7. Network Service utilizes security policy to evaluate workstation credentials and determine type of access. Security policy may be stored on the Network Server or on a Network Policy Server or Directory Server.
Local Workstation Assessment Service
825
800

Figure 8

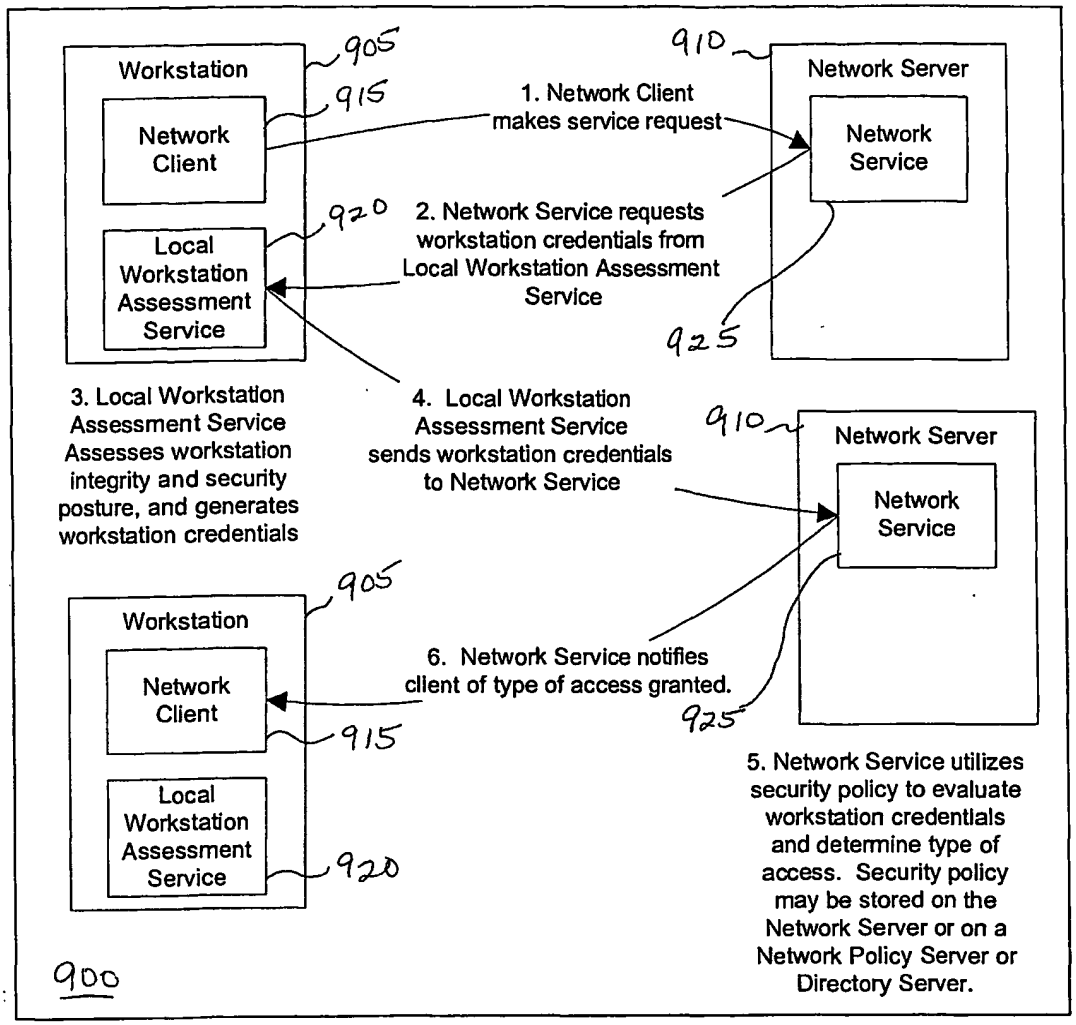

Workstation
905
915
Network Client
920
Local Workstation Assessment Service
910
Network Server
Network Service
1. Network Client makes service request
2. Network Service requests workstation credentials from Local Workstation Assessment Service
925
3. Local Workstation Assessment Service Assesses workstation integrity and security posture, and generates workstation credentials
4. Local Workstation Assessment Service sends workstation credentials to Network Service
910
Network Server
Network Service
905
Workstation
Network Client
915
Local Workstation Assessment Service
920
6. Network Service notifies client of type of access granted.
925
5. Network Service utilizes security policy to evaluate workstation credentials and determine type of access. Security policy may be stored on the Network Server or on a Network Policy Server or Directory Server.
900

Figure 9